

1
2
3
4
5 UNITED STATES DISTRICT COURT
6 WESTERN DISTRICT OF WASHINGTON
7 AT TACOMA

8 UNITED STATES OF AMERICA,

9 Plaintiff,

v.

10 DONNIE BARNES SR.,

11 Defendant.

CASE NO. CR18-5141 BHS

ORDER DENYING
DEFENDANT'S MOTION TO
SUPPRESS

12
13 This matter comes before the Court on Defendant Donnie Barnes, Sr.'s ("Barnes")
14 motion to suppress. Dkt. 32. The Court has considered the pleadings filed in support of
15 and in opposition to the motion and the remainder of the file and hereby denies the
16 motion for the reasons stated herein.

17 **I. PROCEDURAL HISTORY & FACTUAL BACKGROUND**

18 Barnes is charged with one count each of production, distribution, and possession
19 of child pornography. Dkt. 13. Trial is set to commence on October 29, 2019.

20 On April 22, 2019, Barnes filed a motion to suppress and a motion for leave to file
21 an overlength motion. Dkts. 31, 32. On May 6, 2019, the Government responded and
22 filed a motion for leave to file an overlength response. Dkt. 36. On May 16, 2019, Barnes

1 replied and filed a motion for leave to file an overlength reply. Dkts. 39, 40. On May 17,
2 2019, the Government surreplied and filed a motion for leave to surreply. Dkts. 41, 42.

3 **1. Investigation and § 1509 Summons**

4 In February 2018, Special Agent Reese Berg (“Agent Berg”), working for
5 Homeland Security Investigations (“HSI”), a component of the Bureau of Immigration
6 and Customs Enforcement (“ICE,” collectively “ICE-HSI”) began investigating Barnes.
7 Agent Berg’s investigation started after ICE-HSI received a lead from Australian police
8 that an individual using the name “TICK10T012TOCK” had uploaded sexually explicit
9 images of a female minor to a foreign photo-sharing website. Dkt. 1 at 3–4. After viewing
10 the images, an Australian officer obtained a list of internet protocol (“IP”) addresses that
11 “TICK10T012TOCK” used to log onto the photo-sharing website.¹ *Id.* at 6. One of these
12 IP addresses, 73.140.63.12, belonged to internet service provider (“ISP”) Comcast
13 Communications (“Comcast”). *Id.* ¶ 13. A HSI officer issued a summons to Comcast
14 requesting subscriber information for that IP address on February 20, 2018. *Id.* HSI
15 issued the summons under the authority of 19 U.S.C. § 1509(a)(1). Dkt. 36-1 at 6–7.

16 Comcast complied with the summons by providing the subscriber records
17 associated with its IP address. *Id.*, ¶ 14; Dkt. 36-1 at 3 (summons return). Specifically,

18
19 ¹ An IP address is defined as “a unique numerical address identifying each computer on
20 the internet.” *In re Application of U.S. for an Order Authorizing use of A Pen Register & Trap*
21 *On (XXX) Internet Serv. Account/User Name, (xxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 48 (D.
22 Mass. 2005). As detailed in the search warrant application in this case, “[a] device called a router
is used to connect multiple digital devices to the Internet via the public IP addresses assigned (to
the subscriber) by the [Internet Service Provider].” Dkt. 32-2 at 16.

Comcast responded that IP address 73.140.63.12 was assigned to customer K.T., associated with a physical service address in Spanaway, Washington, and that the email user identification for the account was dobsr@comcast.net. Dkt. 36-1 at 3. The extent of the subscriber information provided by Comcast to ICE-HSI is shown in the below image.

Based on the information provided pursuant to the Summons, the subscriber information obtained has been provided below:

Subscriber Name:	K [REDACTED] T [REDACTED]
Service Address:	[REDACTED]
	SPANAWAY, WA 983878237
Telephone #:	[REDACTED]-0983
Type of Service:	High Speed Internet Service
Account Number:	[REDACTED]3402
Start of Service:	Unknown
Account Status:	Active
IP Assignment:	Dynamically Assigned
Current IP:	See Attached
E-mail User Ids:	dobsr
	(The above user ID(s) end in @comcast.net)

Id. Barnes and K.T. live together at the Spanaway address, along with K.T.'s two children. Dkt. 32 at 3.

2. Execution of Search Warrant

After receiving the above internet subscriber information from Comcast, Agent Berg sought a warrant authorizing the search of Barnes's person and home from Magistrate Judge Teresa L. Fricke. Dkt. 32-2. Before applying for the warrant, Agent Berg conducted surveillance on Barnes's home on two dates, February 28 and March 1, 2018. Dkt. 32-2, ¶¶ 22, 25. On February 28, Agent Berg saw K.T. leave the home at 6:30 a.m., accompanied by her two children. *Id.* ¶ 22. On March 1, Agent Berg saw Barnes leave the home at 6:02 a.m. *Id.* ¶ 25

1 Based on Agent Berg’s observations, Judge Fricke found good cause to grant
2 permission to execute the search warrant at night. Dkt. 36-2 at 2 (warrant granting
3 permission to search “at any time in the day or night because good cause has been
4 established”); Fed. R. Crim. P. 41 (defining “daytime” as the hours between 6:00 A.M.
5 and 10:00 P.M.).

6 Law enforcement executed the warrant shortly after 5:00 a.m. on March 6, 2018.²
7 Dkt. 1 ¶ 17. Barnes was home and agreed to speak with Agent Berg. *Id.* During the
8 interrogation Barnes admitted possessing incriminating depictions of K.T.’s minor
9 daughter, which was later corroborated through forensic examination of digital devices
10 seized from the Spanaway residence pursuant to the warrant. *Id.* ¶¶ 17–18; Dkt. 36 at 4.

11 II. DISCUSSION

12 A. Motion to Strike

13 In surreply, the Government asserts that in reply Barnes “raises two matters not
14 previously presented in his opening brief and mischaracterizes the Government’s position
15 on a third.” Dkt. 42. Under local rule, the filing of surreplies in this District is limited to:

16 requests to strike material contained in or attached to a reply brief, in which
17 case the opposing party may file a surreply requesting that the court strike
the material, subject to the following . . .

18 (2) The surreply . . . shall be strictly limited to addressing the request to strike.
19 Extraneous argument or a surreply filed for any other reason will not be
considered.

20
21 ² Each party asserts that the warrant was executed at approximately 5:15 a.m. on March
22 6, 2018, although neither party provides citation to the record regarding the time of execution.
See Dkt. 32 at 14; Dkt. 36 at 3. The Court adopts the parties’ assertion for purposes of this
motion.

1 Local Rule W.D. Wash. LCR 7(g). The Government requests that the Court not consider
2 the two arguments Barnes allegedly raised for this first time in reply. Dkt. 42 at 1–2.
3 Therefore, the Court will construe that part of the Government’s surreply as a motion to
4 strike those arguments from the record, consistent with Local Rule W.D. Wash. LCR 7(g).

5 However, the Government also argues that Barnes’s reply “mischaracterize[d] the
6 Government’s position” regarding the applicability of the good faith exception to the
7 exclusionary rule in this case. Dkt. 42 at 2 (citing Dkt. 40 at 1). The Government presents
8 legal argument in surreply as to why it believes the exception is applicable. Dkt. 42 at 2–
9 3. This is “[e]xtraneous argument” not made in furtherance of a motion to strike and
10 therefore the Court will not consider it. Local Rule W.D. Wash. LCR 7(g). To the extent
11 the Government seeks leave to surreply to respond to Barnes’s mischaracterization of its
12 position, the motion is denied.

13 Turning to the other two arguments, the Court must determine whether Barnes
14 raised for the first time in reply a request for dismissal of count one as an alternative remedy
15 to suppression and a factual argument that he and K.T. jointly possessed the Comcast
16 account. *See* Dkt. 40 at 2–3. Regarding dismissal of count one under the Court’s
17 supervisory powers, the Court finds that Barnes made this request for the first time in reply,
18 cutting off the Government’s ability to respond to the legality of the application of an
19 alternative remedy. Because Barnes failed to request the alternative remedy in his opening
20 brief, he has waived the argument and the court will not consider it. *Zamani v. Carnes*, 491
21 F.3d 990, 997 (9th Cir. 2007) (citing *Koerner v. Grigas*, 328 F.3d 1039, 1048 (9th Cir.
22 2003) (affirming district court after it declined to consider an argument raised for the first

1 time in reply)). The Court therefore grants the motion to strike Barnes's request for an
2 alternative remedy from the reply.

3 Regarding Barnes's argument that he and K.T. shared the Comcast account, Dkt.
4 40 at 2, the Court finds that Barnes presented sufficient detail in his opening brief to
5 negate the Government's assertion that this argument was raised for the first time in
6 reply. The question is close because Barnes neither discussed his alleged interest in the
7 account nor presented facts about his control over the account in his opening brief.
8 *Compare* Dkt. 32 at 2–3 *with* Dkt. 40 at 2–3. The Court ultimately concludes that this
9 argument should not be stricken because although Barnes did not file the summons return
10 from Comcast as an exhibit, in his opening brief he stated that information provided in
11 the return listed the email user associated with the account as “dobsr@comcast.net.” Dkt.
12 32 at 3. Moreover, it was clear from Barnes's opening brief that Barnes lived at the
13 residence and, while not directly stated, used the internet there. *Id.* at 2–3. Because
14 Barnes presented these details in his opening brief, it was appropriate for Barnes to argue
15 in reply that he “shared” the account with K.T., based on their “joint access” to the
16 internet service, their joint payment of the bill, and their “intermingled” account
17 information. Dkt. 40 at 2. Therefore, the Court will consider this argument alongside the
18 Government's challenge to the sufficiency of Barnes's evidentiary support for the
19 argument when analyzing Barnes's standing to assert a Fourth Amendment claim.

20 **B. Motion to Suppress**

21 Barnes moves to suppress all fruits of summonses issued by ICE-HSI and all fruits
22 of the search of his home, including his statements to law enforcement. Dkt. 32 at 1. The

proponent of a motion to suppress has the burden of establishing that his Fourth Amendment rights were violated by a challenged search or seizure. *United States v. Caymen*, 404 F.3d 1196, 1199 (9th Cir. 2005) (citation omitted).

1. Fourth Amendment Violation

Barnes contends that Agent Berg's use of § 1509 summonses was unlawful and violated his Fourth Amendment privacy interest in the internet subscriber information obtained from Comcast. Dkt. 32 at 4–12. The Government responds that (1) Barnes does not have standing to assert a Fourth Amendment claim over an account that is not his; (2) subscriber information associated with a particular IP address is not protected by the Fourth Amendment because customers voluntarily provide this information to their internet service providers; and (3) § 1509 authorized Agent Berg to issue the summons because Comcast's records were relevant to ICE-HSI's investigation of child exploitation offenses. Dkt. 36 at 5–9. The Court concludes that the Government's arguments are dispositive.

A defendant seeking to exclude evidence allegedly obtained in violation of the Fourth Amendment must have standing to challenge the illegal conduct leading to the discovery of the evidence. *Brown v. United States*, 411 U.S. 223, 230 (1973) ("Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.") (citations omitted). The test for whether a defendant's rights are personally violated is "placed within the purview of substantive Fourth Amendment law." *Rakas v. Illinois*, 439 U.S. 128, 140 (1978). Accordingly, a defendant's right to claim the protection of the Fourth Amendment depends upon whether the defendant "has

1 exhibited an actual (subjective) expectation of privacy” in the place searched or the item
2 seized, and further, whether society is prepared to recognize that expectation of privacy
3 as reasonable. *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (internal quotations and
4 alterations omitted). The parties agree that for Barnes to invoke Fourth Amendment
5 protection, he must demonstrate that he has a personal and legitimate expectation of
6 privacy in the subscriber information associated with the Comcast account at issue.

7 **a. Barnes’s Expectation of Privacy in the Comcast Account**

8 The Government contends that Barnes cannot challenge Agent Berg’s acquisition
9 of the internet subscriber information at issue because the subscriber account “does not
10 belong to him.” Dkt. 36 at 6. The Court agrees that it is difficult for Barnes to
11 demonstrate that he has a subjective expectation of privacy in the Comcast account. First,
12 it is undisputed that K.T. is the sole subscriber on the Comcast account. Dkt. 36-1 at 3.
13 Comcast assigned K.T. an IP address, and it was this IP address, assigned to K.T. as the
14 account holder, that led Agent Berg to K.T. and Barnes’s shared residence. It is thus
15 doubtful that Barnes has demonstrated that “he personally has an expectation of privacy”
16 in the seized items, *Minnesota v. Carter*, 525 U.S. 83, 88 (1998), that is, in K.T.’s internet
17 subscriber information held by Comcast.

18 While Barnes concedes that the account was “nominally” K.T.’s, Dkt. 40 at 2, he
19 argues that he has standing to challenge the seizure because he and K.T. shared “joint-
20 residential usage” of the internet and that the account information was “intermingled.” *Id.*
21 Barnes compares his interest in the account to that of an overnight social guest, where a
22 defendant may have standing to challenge a search of a third-party residence upon a

1 showing of joint control or common authority of the residence. *Id.* (citing *Minnesota v.*
2 *Olson*, 495 U.S. 91 (1990) and *United States v. Grandberry*, 730 F.3d 968, 974 (9th Cir.
3 2013)). However, although incriminating evidence was ultimately obtained from
4 Barnes’s home, the expectation of privacy that Barnes must demonstrate now is in the
5 Comcast subscriber records at issue, Dkt. 36-1 at 3. Barnes does not explain how the
6 Fourth Amendment’s fundamental protection of an individual’s privacy interest in the
7 *home*, relied on by the *Olson* and *Grandberry* courts in reaching their respective
8 holdings, extends to his privacy interest in internet subscriber records held by an ISP. *See*
9 *Olson*, 495 U.S. at 98–100 (recognizing that overnight social guests have a legitimate
10 expectation of privacy in the homes of their hosts); *Grandberry*, 730 F.3d at 982
11 (declining to extend provision allowing parole officers to search property under
12 defendant’s control to a third party’s home in part because it would threaten “the privacy
13 interests of non-parolees in the home, where Fourth Amendment rights are ‘sacrosanct’”) (citation omitted). Barnes’s authorities thus do little to advance his claimed expectation
14 of privacy in the Comcast account.
15

16 Similarly, Barnes’s attempt to establish standing by asserting that the account was
17 jointly held is negated by (1) Comcast’s summons return showing that the account was
18 held solely by K.T., *see* Dkt 36-1 at 3; and (2) his failure to submit any actual evidence
19 documenting his alleged authority or control over the account. Although Barnes tries to
20 assert facts establishing his control over the account, unsworn assertions made by
21 attorneys in pleadings are not evidence. It is thus doubtful that Barnes has even
22 demonstrated a subjective expectation of privacy in the account, let alone a legitimate one

1 that society is prepared to recognize as reasonable. In any event, there is an absence of
2 evidence to establish standing. Therefore, the Court concludes that Barnes has not shown
3 that he has a personal expectation of privacy in K.T.'s Comcast account.

4 **b. Barnes's Expectation of Privacy in Internet Subscriber Records**

5 Barnes's claim of a personal violation of his rights is further undermined by an
6 examination of the protection granted to internet subscriber records under the Fourth
7 Amendment. It is well-settled that "a person has no legitimate expectation of privacy in
8 information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743–44
9 (citations omitted). Here, the only reason Comcast possessed the identifying subscriber
10 data at issue is because it had been voluntarily provided to the company by K.T. Her
11 subscriber information was the only information Agent Berg requested (and Comcast
12 provided) via summons. Dkts. 32-3 at 3 (summons), 36-1 at 3 (summons return). Because
13 K.T. provided her subscriber information to third-party Comcast voluntarily, Barnes's
14 claimed expectation of privacy in the subscriber information fails under *Smith*. Indeed,
15 "[e]very federal court to address this issue has held that subscriber information provided
16 to an internet provider is not protected by the Fourth Amendment's privacy expectation."
17 *United States v. Perrine*, 518 F.3d 1196, 1204–05 (10th Cir. 2008); *see also United States*
18 *v. Corbitt*, 588 F. App'x 594 (9th Cir. 2014); *United States v. Wheelock*, 772 F.3d 825,
19 828–29 (8th Cir. 2014); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010); *Guest*
20 *v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001).

21 Barnes, noting that this Circuit's unpublished precedent on the issue is non-
22 binding, nevertheless invites a different conclusion by asserting that IP addresses

1 implicate “similar, if not greater, privacy interests” than cell phone location history
2 (“CSLI”). Dkt. 32 at 9–11 (relying on *United States v. Carpenter*, 138 S. Ct. 2206, 2217
3 (2018) (finding legitimate expectation of privacy in defendant’s physical movements as
4 shown through CSLI).³ Barnes’s reliance on *Carpenter* is premature because the decision
5 explicitly declined to overrule the third-party doctrine, which is dispositive to this issue.
6 *Carpenter*, 138 S. Ct. at 2220 (“We do not disturb the application of *Smith* and *Miller* . . .
7 nor do we address other business records that might incidentally reveal location
8 information.”).⁴ Moreover, analogizing to the pen register device at issue in *Smith*, the
9 Circuit held in a 2008 decision that “Internet users have no expectation of privacy in . . .
10 the IP addresses of the websites they visit because they should know that this information
11 is provided to and used by Internet service providers for the specific purpose of directing
12 the routing of information.” *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir.
13 2008). *Corbitt*, the Circuit’s 2014 memorandum decision on the issue, cites to the
14 published decision *Forrester* for this point. *Corbitt*, 588 F. App’x at 595. The Court is
15 therefore without justification to conclude under existing precedent that Barnes holds a
16

17
18 ³ CLSI is information automatically generated every time a cell phone connects to cell
19 towers, which cell phones do autonomously and almost continuously to find and maintain the
20 best signal. Wireless carrier companies record this information for business purposes. *Carpenter*,
138 S. Ct. at 2211–12. The Supreme Court expressed concern that CSLI provides “a detailed
chronicle of a person’s physical presence compiled every day, every moment, over several
years.” *Id.* at 2220.

21 ⁴ The Court was referring to *Smith* and *United States v. Miller*, 425 U.S. 435 (1976), the
22 cases which established that “a person has no legitimate expectation of privacy in information he
voluntarily turns over to third parties.” *Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 442–44.

1 legitimate expectation of privacy in subscriber information, including IP addresses
2 assigned by an ISP to a particular customer account, that the Fourth Amendment will
3 protect.

4 In sum, Barnes fails to show he had a legitimate expectation of privacy in the
5 subscriber information resulting in a personal violation of his rights for two reasons: (1)
6 the subscriber account from which the information was seized belonged to someone else;
7 and (2) the account holder voluntarily provided her subscriber information to Comcast
8 during the course of her customer relationship with the company. Therefore, the
9 Government did not violate the Fourth Amendment when Agent Berg obtained K.T.'s
10 internet subscriber information from Comcast via a § 1509 summons.

11 **2. Statutory Violation**

12 Next, Barnes asserts that § 1509 summonses may only be used for investigations
13 ensuring compliance with customs laws such as the collection of duties, fees, and taxes,
14 and by issuing a § 1509 summons to investigate a criminal child pornography offense,
15 ICE-HSI exceeded its authority and violated the statute. Dkt. 32 at 4–8. Barnes also
16 argues that suppression is warranted because agents routinely issued § 1509 summonses
17 improperly, resulting in a pattern of widespread statutory violations of constitutional
18 magnitude. *Id.* at 12–14. The Government contends that § 1509 “authorized the summons
19 to Comcast” in connection to ICE-HSI’s authority to investigate child exploitation
20 offenses. Dkt. 36 at 9–13.

21 19 U.S.C. § 1509 provides that a summons may issue:
22

1 In *any investigation or inquiry* conducted for the purpose of ascertaining the
2 correctness of any entry, for determining the liability of any person for duty,
3 fees and taxes due or duties, fees and taxes which may be due the United
4 States, for determining liability for fines and penalties, or for *insuring*
5 *compliance with the laws of the United States administered by the United*
6 *States Customs Service*, the Secretary (but no delegate of the Secretary below
7 the rank of district director or special agent in charge) may—

8 (1) examine, or cause to be examined, upon reasonable notice, *any record*
9 (which for purposes of this section, includes, but is not limited to, any
10 statement, declaration, document, or electronically generated or machine
11 readable data) described in the notice with reasonable specificity, which *may*
12 *be relevant* to such investigation or inquiry.

13 19 U.S.C. §§ 1509(a)–(a)(1) (emphasis added). Therefore, the plain language of § 1509
14 grants the United States Customs Service the authority to issue summonses for records
15 that “may be relevant” to “any” investigation conducted to ensure compliance with the
16 laws that the Customs Service administers. § 1509(a)(1).

17 ICE-HSI now holds the authority of the former Customs Service. The Homeland
18 Security Act of 2002 shifted the functions of the Customs Service to the Department of
19 Homeland Security, 6 U.S.C. § 203, and divided the Customs Service “into the Bureau of
20 Customs and Border Protection and the Bureau of Immigration and Customs
21 Enforcement,” *United States v. Reyeros*, 537 F.3d 270, 274 n.2 (3d Cir. 2008). As a
22 component of ICE, ICE-HSI is part of the Department of Homeland Security. *See id.*
Thus, § 1509 authorizes ICE-HSI to issue summonses to ensure compliance with the laws
of the United States that it administers.

As the Government explains, ICE-HSI routinely administers investigations into
child exploitation offenses to ensure compliance with United States law. Indeed, ICE
maintains a Child Exploitation Investigations Unit that is tasked by statute with

1 coordinating all of ICE’s “child exploitation initiatives,” which includes investigations
2 into child pornography and child exploitation. Dkt. 36 at 10–11 (citing 6 U.S.C. §
3 473(b)(1)–(2)). At least two other courts have approved ICE-HSI’s use of § 1509
4 summonses to investigate offenses against children based on this well-documented role.
5 *See United States v. Cray*, 673 F. Supp. 2d 1368, 1377 (S.D. Ga. 2009) (citing *Hallock v.*
6 *United States*, 253 F. Supp. 2d 361, 365 (N.D. N.Y. 2003) (upholding use of § 1509
7 summons because ICE “has had substantial duties in investigating and serving search
8 warrants upon alleged purveyors of child pornography.”)); *United States v. Merrell*, 88 F.
9 Supp. 3d 1017, 1033 (D. Minn. 2015) (upholding use of § 1509 summons after finding
10 that ICE agent was “tasked with investigating violations of [production of child
11 pornography].”), *aff’d* 842 F.3d 577 (8th Cir. 2016). Because ICE-HSI is tasked with
12 investigating child exploitation, the Court concludes that the § 1509 summonses issued
13 here furthered “a legitimate investigative purpose in compliance with the statute.” *Cray*,
14 673 F. Supp. 2d at 1377. Barnes therefore fails to show that ICE-HSI violated § 1509.

15 Further, the Court concludes that even if § 1509 did not authorize the summons,
16 exclusion of evidence is inappropriate to remedy what would only be a statutory violation
17 of non-constitutional magnitude. It is well-settled that while exclusion is a proper remedy
18 for some Fourth Amendment violations, there is no exclusionary rule generally applicable
19 to statutory violations. *See Herring v. United States*, 555 U.S. 135, 139–40 (2009) (citing
20 *United States v. Calandra*, 414 U.S. 338, 348 (1974) (the exclusionary rule is “designed
21 to safeguard Fourth Amendment rights generally through its deterrent effect.”)); *see also*
22 *Davis v. United States*, 564 U.S. 229, 237–38 (2011) (finding “heavy toll” of suppression

1 appropriate only when law enforcement officials act in “‘deliberate,’ ‘reckless,’ or
2 ‘grossly negligent disregard for Fourth Amendment rights.’”). Thus, “the application of
3 [the exclusionary rule] is appropriate when the Constitution or a statute requires it.”
4 *United States v. Abdi*, 463 F.3d 547, 555 (6th Cir. 2006) (citations omitted).

5 Here, neither the Constitution nor § 1509 require suppression. In the “few cases”
6 where the Supreme Court has suppressed evidence based on a statutory violation, they
7 have done so because “the excluded evidence arose directly out of statutory violations
8 that implicated important Fourth and Fifth Amendment interests.” *Sanchez-Llamas v.*
9 *Oregon*, 548 U.S. 331, 348 (2006) (quoting *Herring*, 555 U.S. at 144). Thus, suppression
10 may be appropriate if ICE-HSI’s alleged violation of § 1509 implicated Barnes’s Fourth
11 Amendment interests. The Court has already found that internet subscriber information
12 held by an ISP, and Barnes’s personal interest in the account, is not subject to the Fourth
13 Amendment’s privacy expectation. Thus, while § 1509 deals generally with evidence
14 gathering, Barnes’s Fourth Amendment rights are not implicated by the alleged statutory
15 violation.

16 Nor does the statute mandate suppression. As the Government asserts, § 1509
17 itself provides no suppression remedy. Dkt. 36 at 14 (citing *United States v. Smith*, 155
18 F.3d 1051, 1056 (9th Cir. 1998) (noting that government violations of the Electronic
19 Communications Privacy Act would not warrant suppression because the statute does not
20 itself provide suppression as a remedy)). Absent the implication of a constitutional right,
21 violations of § 1509 alone do not warrant the exclusion of the evidence. Therefore,
22 Barnes is not entitled to suppression of the evidence even if the Court were to conclude

1 that ICE-HSI exceeded its statutory authority by issuing § 1509 summonses to investigate
2 child pornography offenses. Accordingly, Barnes's motion to suppress the fruits of the
3 § 1509 summons is denied.

4 **3. Nighttime Search Warrant Provision**

5 Finally, Barnes argues that fruits of the search of his home should be suppressed
6 because Agent Berg's affidavit provided insufficient justification to support the issuance
7 of a nighttime search warrant, and therefore the nighttime search violated the Fourth
8 Amendment. Dkt. 32 at 14–18. The Government counters that Agent Berg complied with
9 Rule 41 of the Federal Rules of Criminal Procedure ("Rule 41") by obtaining Judge
10 Fricke's express permission to search at night upon a finding of good cause and that in
11 any case, execution of the warrant shortly after 5:00 a.m. was objectively reasonable.
12 Dkt. 36 at 16–19.

13 The Fourth Amendment does not contain any time limitations on reasonable
14 searches and seizures. *See* U. S. Const. amend. IV. However, Rule 41 provides that
15 warrants must be executed "during the daytime" unless the issuing judge authorizes
16 execution at another time upon a showing of good cause. Fed. R. Crim. P. 41(e)(2)(A)(ii).
17 Daytime is defined as "the hours between 6:00 a.m. and 10:00 p.m." local time. Fed. R.
18 Crim. P. 41 (a)(2)(B).

19 In addition to describing Agent Berg's surveillance of the home, the affidavit
20 submitted in support of the nighttime search provision stated as follows:

21 As part of this application, I am seeking authority to execute this warrant
22 before 6:00 a.m. Given the observations of the SUBJECT PERSON's morning routine described above, I believe they may depart for work prior

1 to or near 6:00 a.m. **I would prefer to execute this warrant while all**
2 **occupants of the SUBJECT PREMISES are present.** To maximize the
3 chances of that being the case, I hope to execute this warrant between 4:00
4 and 6:00 a.m.

5 Dkt. 32-2 at 15, ¶ 26. Thus, Agent Berg's stated "cause" for executing the warrant prior
6 to 6:00 a.m. was his "preference" to do so while Barnes, and the rest of the home's
7 occupants, were together in one place at the residence. *Id.*

8 To assess whether this justification constitutes good cause, Barnes argues for "a
9 clear showing of particularized need" standard. Dkt. 32 at 17 (citing Wayne LaFave, 2
10 Search & Seizure § 4.7(b) (5th ed.) ("it is submitted that the true test of the
11 constitutionality of a nighttime search is whether it was necessary to make the search at
12 that time.")). The Government counters that Agent Berg's affidavit established good cause
13 for the search that Barnes fails to negate with authority, *id.* at 16–17, and that "the
14 daytime requirement for search warrants does not come from the Fourth Amendment
15 itself, which requires only reasonableness," *id.* at 16.

16 The Court notes that it is hindered by the dearth of authority assessing what
17 constitutes "good cause" for a nighttime search under Rule 41. In the affidavit, Agent
18 Berg sought permission to search the home at night upon a showing that (1) it was
19 preferable to execute the warrant while all residents of the home were present; and (2) the
20 suspect and other occupants of the home frequently departed early in the morning,
21 thwarting the goal of a unified search during the time when Agent Berg could have
22 executed the warrant without any special judicial authorization under Rule 41. Dkt. 32-2
at 14–15. Agent Berg did not explain *why* it was preferable, necessary, or justified to

1 search when all residents were present. *Id.* On this showing, Judge Fricke found good
2 cause to search at night, which is all that is required by Rule 41. Dkt. 36-2 at 2.

3 Whether review of Judge Fricke’s good cause finding is de novo or discretionary,
4 when substituting its own view, the Court also concludes that the affidavit established
5 good cause to execute the warrant when all residents were at home. Because a search
6 when all residents were home was unlikely to occur if the search took place after 6:00
7 a.m., it was appropriate to authorize the occurrence of the search before 6:00 a.m. based
8 on Agent Berg’s preference to do so.⁵ Because the affidavit provided good cause for a
9 search outside the hours permitted by Rule 41, law enforcement did not violate the rule
10 when they executed the warrant on Barnes’s residence on March 6, 2018.

11 Moreover, even if the Court is incorrect in concluding that good cause justified the
12 timing of the search, suppression to remedy a Rule 41 violation is proper only if

13 1) the violation rises to a “constitutional magnitude;” 2) the defendant was
14 prejudiced, in the sense that the search would not have occurred or would not
15 have been so abrasive if law enforcement had followed the Rule; or 3)
16 officers acted in “intentional and deliberate disregard” of a provision in the
17 Rule.

18 *United States v. Williamson*, 439 F.3d 1125, 1133 (9th Cir. 2006) (citing *United*
19 *States v. Martinez-Garcia*, 397 F.3d 1205, 1213 (9th Cir. 2005); *United States v.*
20 *Crawford*, 657 F.2d 1041, 1047 (9th Cir. 1981)). The Court does not find that Barnes
21 suffered prejudice because he answered the door when officers began executing the

22 ⁵ Although Agent Berg used the word “prefer,” the Court concludes that this statement of
preference implies a factual basis for a search by law enforcement that is reasonable—that is, a
search that assures the possessor of the residence is present, which in most circumstances is
preferable to searches conducted when an owner is not present.

1 warrant, and when the search would still have occurred even if Judge Fricke had not
2 authorized it to begin prior to 6:00 a.m. There is also no evidence that Agent Berg
3 deliberately disregarded Rule 41 when he sought (and received) Judge Fricke's express
4 authorization to begin the search before 6:00 a.m. And, Barnes fails to demonstrate with
5 authority that execution of the warrant at 5:15 a.m. rendered the search unreasonable
6 under the Fourth Amendment, meaning any alleged violation is not of constitutional
7 magnitude. Therefore, Barnes has not demonstrated any violation of Rule 41 that
8 warrants suppression as a remedy.

9 Finally, even if the early morning execution of the warrant did render the search
10 unreasonable under the Fourth Amendment, suppression remains unavailable. Under the
11 good-faith exception to the exclusionary rule announced in *United States v. Leon*, 468
12 U.S. 897, 920–21 (1984), evidence should not be excluded to remedy a constitutional
13 violation when officers rely in good faith on a search warrant issued by a neutral and
14 detached magistrate.⁶ As discussed above, there is no evidence that any potential
15 violation of either the rule or the Fourth Amendment was deliberate or the result of bad
16 faith. Nor does the Court find that the affidavit was so “bare bones” as to render Agent
17 Berg's good faith reliance on the warrant objectively unreasonable. *Leon*, 468 U.S. at

18
19 ⁶ Barnes disputes the applicability of the good faith exception where the alleged Fourth
20 Amendment violation stems from the *execution*, and not the validity of, a warrant. Dkt. 17 at 4
21 (citing *United States v. Gantt*, 194 F.3d 987, 1006 (9th Cir. 1999), *reversed on other grounds by*
22 *United States v. W.R. Grace*, 526 F.3d 499 (9th Cir. 2008)). However, the Court finds the
application of *Leon* appropriate because Agent Berg's alleged violation of Rule 41 arises out of
his reliance on the validity of the judicial officers' determination of good cause to execute the
warrant before 6:00 a.m., akin to the circumstances confronted by the *Leon* court. 468 U.S. at
922.

1 915. Because police here held an objectively reasonable belief in the validity of the
2 warrant authorizing the nighttime search, “excluding the evidence will not further the
3 ends of the exclusionary rule in any appreciable way; for it is painfully apparent that . . .
4 the officer is acting as a reasonable officer would and should act in similar
5 circumstances.” *Leon*, 468 U.S. at 920 (quoting *Stone v. Powell*, 428 U.S. 465, 539–540
6 (1976) (White, J., dissenting)). The Court therefore declines to suppress the evidence
7 even if executing the warrant shortly after 5:00 a.m. violated the Fourth Amendment.
8 Accordingly, Barnes’s motion to suppress the fruits of the search of his home is denied.

9 **C. Remaining Motions**

10 The Court has reviewed the parties’ motions to file overlength motions, responses,
11 and replies. Dkts. 31, 35, 39. The Court agrees that the nature of the issues presented in
12 the motion necessitated the filing of pleadings longer than the page limits authorized by
13 Local Rule W.D. Wash. CrR 12(b)(5). Therefore, the Court grants each motion.

14 **III. ORDER**

15 Therefore, it is hereby **ORDERED** that Barnes’s motion to suppress, Dkt. 32, is
16 **DENIED**. The parties’ motions for leave to file overlength pleadings, Dkts. 31, 35, 39,
17 are **GRANTED**. The Government’s motion for leave to surreply, Dkt. 41, is **GRANTED**
18 **in part**.

19 Dated this 18th day of June, 2019.

20
21 

22 BENJAMIN H. SETTLE
United States District Judge